The Current State of HIPAA:

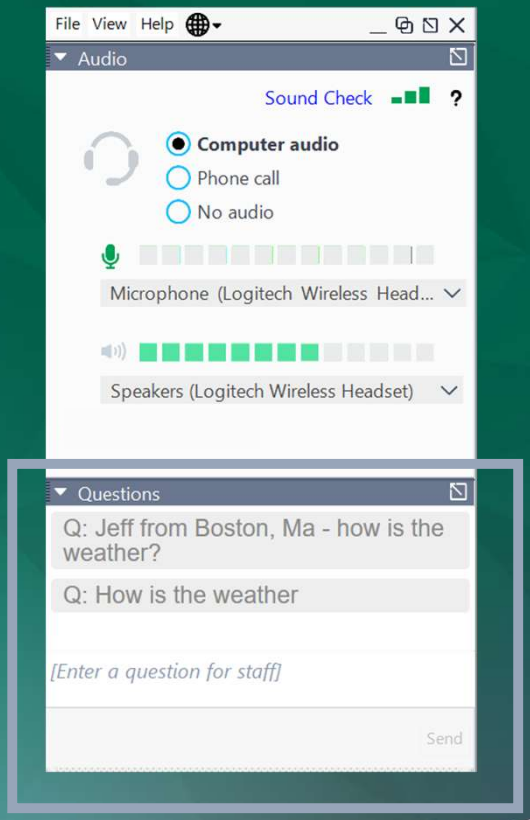
Reviewing Our 2024 HIPAA Compliance Benchmark Survey Results

SAI360

STRATEGIC MANAGEMENT SERVICES

Questions or Feedback?

Please type your questions or comments in the "Questions" tab.



SAI360

STRATEGIC MANAGEMENT SERVICES

This Event Is Approved For CCB Credits

CCB Compliance Certification Board — APPROVED FOR 1.2 CCB CREDIT(s)

The Compliance Certification Board (CCB)® has approved this event for up to 1.2 live CCB CEUs. Continuing Education Units are awarded based on individual attendance records. Granting of prior approval in no way constitutes endorsement by CCB of this event content or of the event sponsor.

adam.winand@sai360.com

TO REQUEST CREDITS

STRATEGIC MANAGEMENT SERVICES

SAI360

2025 HIPAA Benchmark Report

Listed under the ‘Documents’ tab

SAI360

STRATEGIC MANAGEMENT SERVICES

WHO WE ARE

STRATEGIC MANAGEMENT SERVICES

has provided HIPAA and compliance advisory services for over 25 years to more than 2,000 organizations, including development and evaluation of HIPAA compliance programs, policies and procedures, training, breach assessments, state and local regulatory compliance, and security risk assessments, as well as overall compliance services that include claims data analyses, arrangement reviews, assistance with CIAs, acting as IROs and Board Compliance Experts, and litigation support.

CRC COMPLIANCE RESOURCE CENTER

operates hotline services, sanction checking and resolution services, compliance surveys, and a compliance related document development and training program.

SAI360

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance software and Ethics & Compliance Learning resources. SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.

TODAY'S PRESENTERS

Robbi-Lynn Watnik
Senior Consultant,
Strategic Management Services

Natalie Lesnick
Consultant,
Strategic Management Services

AGENDA

- Survey Introduction
- HIPAA Program Structure, Responsibility and Oversight
- HIPAA Program Operations, Policies, Training, and Business Associates
- HIPAA Investigations, Breach Management, and Audits
- HIPAA Program Planning, Priorities and Audits
- Enforcement
- Overall Conclusion
- Q&A Session

STRUCTURE OF SURVEY

- 31 survey questions.
- 227 survey respondents.
- Nearly half of respondents reported being associated with a hospital or health system, while others were associated with behavioral/mental health, physician/group practice, health plan/insurance provider, skilled nursing/long-term care, and clinic/ambulatory surgery center.
- There was a significant increase in respondents associated with behavioral/mental health.
- Respondents were dispersed over a variety of health care provider types or vendors (i.e., home health, laboratory, pharmacy, etc.).

SURVEY GOALS

- The nature and level of commitment that healthcare organizations have made to HIPAA compliance in 2024
- HIPAA training frequency and enforcement
- HIPAA audit areas
- Enforcement encounters entities have experienced
- Potential HIPAA priorities for organizations

FOR IMMEDIATE RELEASE
January 15, 2025

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for $10,000

Settlement with Northeast Surgical Group marks OCR's 10th ransomware enforcement action and 4th enforcement action in OCR's Risk Analysis Initiative.

Today the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a settlement with Northeast Surgical Group, P.C. (NESG), a provider of surgical services in Michigan, for a potential violation under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules, which set forth the requirements that covered entities (health plans, health care clearinghouses, and most health care providers), and business associates must follow to protect the privacy and security of protected health

DEPARTMENT OF HEALTH & HUMAN SERVICES
Office for Civil Righ

FOR IMMEDIATE RELEASE
December 3, 2024

Contact: HHS Press Office
202-690-6343
media@hhs.gov

HHS Office for Civil Rights Imposes a $1.19 Million Penalty Against Gulf Coast Pain Consultants for HIPAA Security Rule Violations

Systemic HIPAA Security Rule violations lead to OCR's 6th penalty of the year

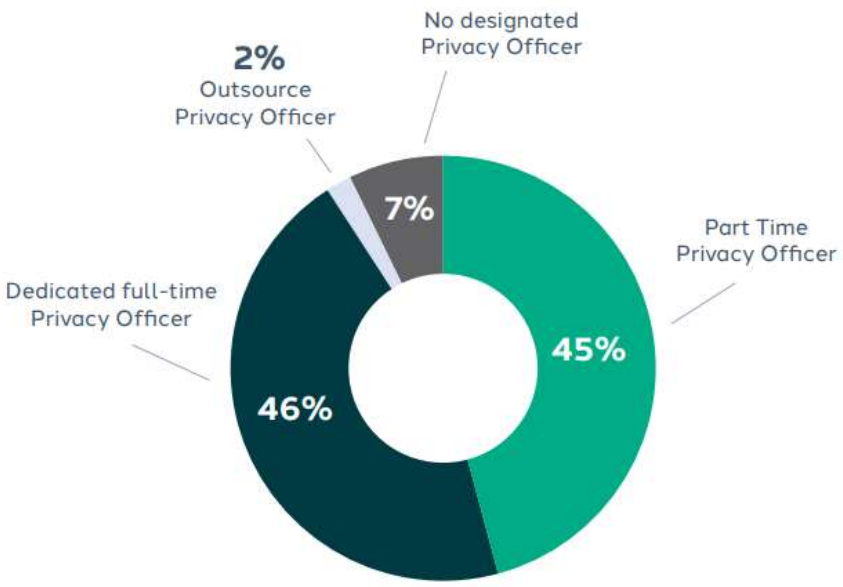
Today, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) announced a $1.19 million civil monetary penalty against Gulf Coast Pain Consultants, LLC d/b/a Clearway Pain Solutions Institute (Gulf Coast Pain Consultants) in Florida, concerning violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, following receipt of a breach report that a former contractor for the company had impermissibly accessed their electronic record system. OCR enforces the HIPAA Privacy, Security, and Breach Notification Rules, which set forth the requirements that health plans, health care clearinghouses, and most health care providers, and their business associates must follow to protect the privacy and security of protected health information (PHI). The HIPAA Security Rule establishes

STRATEGIC MANAGEMENT

HIPAA Program Structure, Responsibility, and Oversight

SAI360

WHICH BEST DESCRIBES YOUR HIPAA PRIVACY OFFICER SITUATION AT YOUR ORGANIZATION?



DISCUSSION:

- A higher percentage of respondents indicated that their organization did not have a designated Privacy Officer.
- Remember: the HIPAA Privacy Rule requires covered entities to designate a privacy officer.
- OCR has stated that the privacy rule is “scalable” so that providers can tailor the program based on their size.
- Providers are advised to be cautious to make sure they meet basic HIPAA Privacy requirements.

WHAT IS THE STAFFING LEVEL FOR THE HIPAA PRIVACY OFFICE FUNCTION?

DISCUSSION:

- Decreases in percentage of full-time privacy officer function may be attributed to an increase in behavioral health organizations.
- The HIPAA Privacy Rule requires a covered entity to “designate a privacy official who is responsible” for HIPAA compliance.
- The rule does not specifically require the amount of time that this individual is expected to devote to their role as the HIPAA Privacy Officer.
- Not having a full-time privacy officer is a risk, especially for larger organizations.
- It is advisable to have an individual with the expertise and bandwidth to properly deal with all privacy issues.

TO WHOM DOES YOUR PRIVACY OFFICER DIRECTLY REPORT?

DISCUSSION:

- OCR nor the regulations specify to whom a privacy officer should report.
- It remains advisable that the Privacy Officer have a direct reporting relationship with the highest level within an organization.

TO WHAT OVERSIGHT COMMITTEE DOES THE PRIVACY OFFICER PROVIDE FORMAL REPORTS?

DISCUSSION:

62%

Over **62%** of respondents indicated that the Privacy Officer provides formal reports directly to the Board of Directors or Board Compliance Committee, which is a higher percentage than our previous survey.

54%

54% of respondents reported that the Privacy Officer provides formal reports to the Executive-level Compliance Committee, which is significantly higher than our previous survey.

21%

Almost **21%** noted that the Privacy Officer provides formal reports to the Executive-level HIPAA Privacy/ Security Committee. This is also higher than the previous survey.

8%

Over **8%** of respondents noted that their organization did not have an oversight body for HIPAA operations, which is a lower percentage than our previous survey.

WHICH OF THE FOLLOWING STATEMENTS BEST DESCRIBES THE SUPPORT RECEIVED FROM YOUR EXECUTIVE LEADERSHIP AND BOARD?

DISCUSSION:

- The combined percentage of “very supportive” and “supportive” executive leadership and Board is a slight decrease over the 2023 survey results.
- Similarly, the combined percentage of weak or nonsupport is slightly higher.
- This is inconsistent with the trend of organizational leadership taking HIPAA Privacy issues seriously.
- This is vital to reduce the potential for HIPAA Privacy violations and subsequent fines.

STRATEGIC MANAGEMENT

HIPAA Program Operations – Policies, Training and Business Associates

SAI360

HOW MANY HIPAA-RELATED POLICIES AND PROCEDURES DOES YOUR ORGANIZATION HAVE?

28%

Almost **28%** have more than 20 HIPAA policies and procedures.

13%

13% have 16-20.

14%

Almost **14%** have 11-15.

17%

Over **17%** have 6-10.

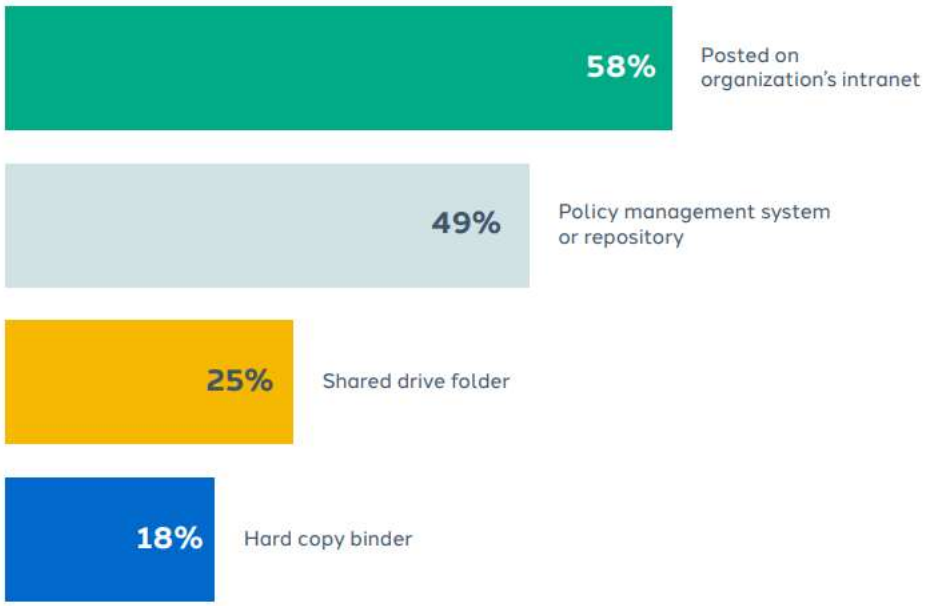
15%

Over **15%** have 1-5.

DISCUSSION:

- Based on HIPAA regulatory requirements, a covered entity is advised to have at least 15 single-topic policies.
- Less than 50% reported having at least 16 or more policies.
- Anything lower indicate that the organization is not fully addressing the Privacy Rule requirements.

HOW DOES YOUR WORKFORCE ACCESS HIPAA-RELATED POLICIES AND PROCEDURES?



DISCUSSION:

- A majority of respondents rely on electronic means for employees to access HIPAA-related policies and procedures.
- The percentage of respondents who continue to make policies available in paper format is a significant increase from our previous survey.

HOW OFTEN DO YOU CONDUCT HIPAA COMPLIANCE TRAINING WITH YOUR EMPLOYEES?

DISCUSSION:

- While slightly lower, these responses are not significantly different from the 2023 survey.
- There is continued evidence that organizations recognize that education is key.
- It is a best practice to provide training to workforce members when hired and at least annually.
- There is also no specific regulatory requirement for annual training, only workforce members must be trained “as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.”

WHAT IS THE FORMAT OF THE TRAINING?

71%

More than **71%** of respondents reported using a learning module.

25%

Over **25%** responded that the training was provided live/in person.

33%

33% use a combination of live and virtual training.

2%

Less than **2%** of respondents reported they were not conducting any training.

DISCUSSION:

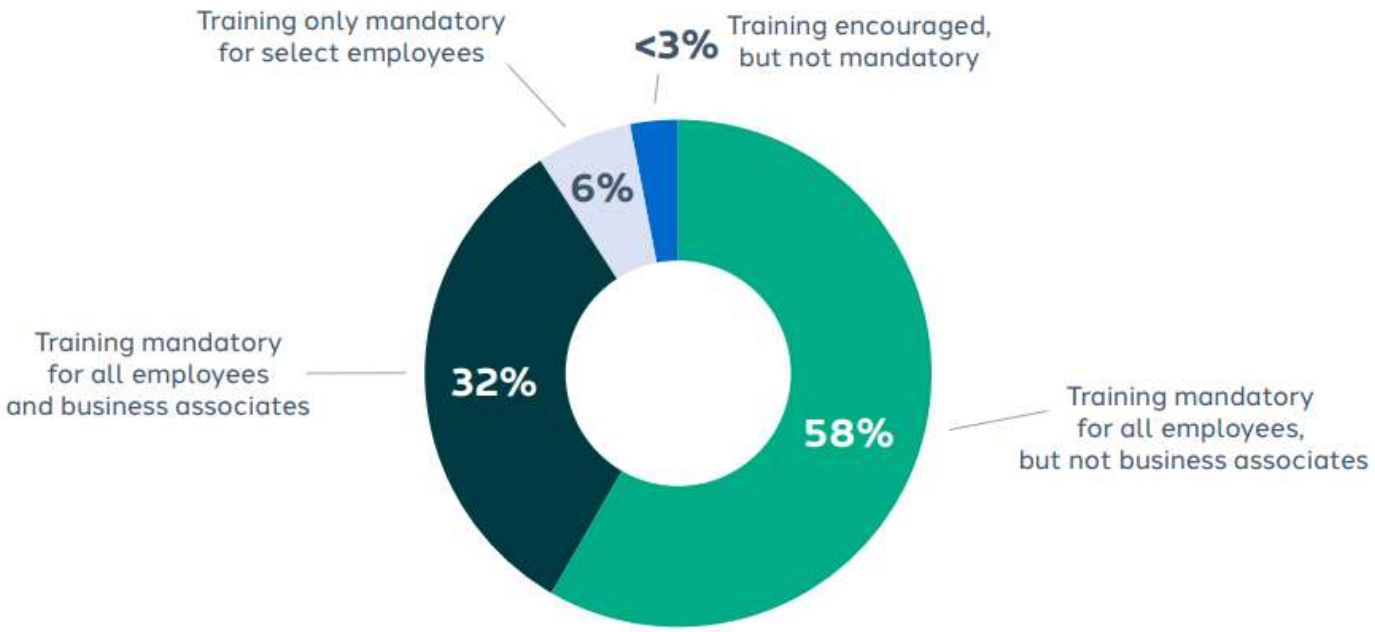
- The majority of respondents use a learning module system when conducting privacy training.
- While more efficient, learning modules do not always allow customization of training.
- A combination of live and virtual training may be a solution for employees to be engaged.

WHAT TYPE OF INFORMATION DOES YOUR ORGANIZATION MAINTAIN FOR HIPAA TRAINING?

DISCUSSION:

IS HIPAA TRAINING MANDATORY FOR ALL EMPLOYEES AND BUSINESS ASSOCIATES (I.E., IS DISCIPLINARY ACTION TAKEN IF THE TRAINING IS NOT COMPLETED?)

DISCUSSION:



ARE THERE CONSEQUENCES IF AN EMPLOYEE OR BUSINESS ASSOCIATE DOES NOT COMPLETE TRAINING?

77%

77% of respondents indicated that employees may be disciplined for noncompletion of training.

22%

22% indicated that a business associate may be terminated for failure to evidence HIPAA training completion.

16%

16% indicated that employees do not face disciplinary action for failing to complete HIPAA training.

10%

Less than **10%** ndicated that business associates are not terminated for failing to evidence completion of HIPAA training.

DISCUSSION:

- Regulations require that all members of a covered entity's workforce receive HIPAA training.
- Business Associates are included in this expectation.
- Best practice: If an individual or business associate does not evidence training completion, there should be some remediation to resolve the noncompletion.

DO YOU MAINTAIN AN INVENTORY OF ALL YOUR BUSINESS ASSOCIATES (E.G., INSURERS, CONSULTANTS, OFF-SITE STORAGE, COPIER/SHREDDING VENDORS, CLOUD PROVIDERS)?

75%

DISCUSSION:

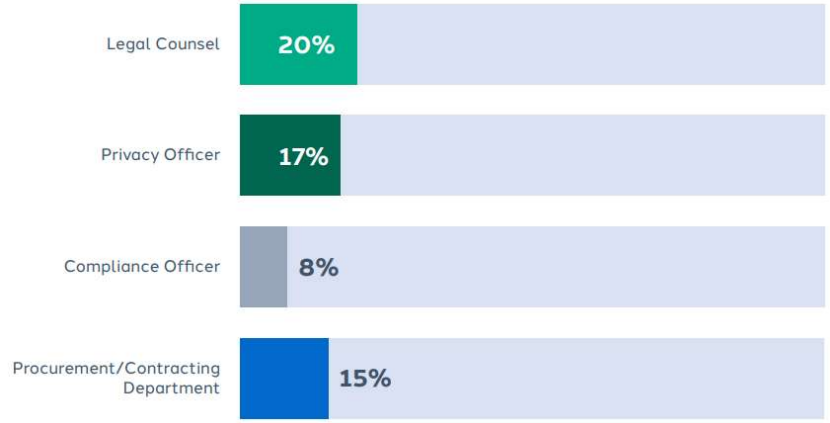
- Maintaining a list of business associates is not a specific HIPAA requirement.
- It is a best practice and can save the covered entity time if OCR chooses the entity for a random audit.
- When this occurs, OCR will ask the covered entity to identify their business associates with contact information.

DO YOU EXECUTE/MAINTAIN CURRENT BUSINESS ASSOCIATE AGREEMENTS (AS REQUIRED UNDER HIPAA) WITH YOUR BUSINESS ASSOCIATES?

DISCUSSION:

- Having an agreement in place with identified BAs is important to protect against unauthorized disclosures of PHI.
- It is also a regulatory requirement and can lead to hefty fines if missing.
- Covered entities are advised to have a checklist in place to identify which vendors meet the definition of a BA and execute an agreement containing at a minimum, the elements in the regulation.

WHO IS RESPONSIBLE FOR MAKING THE FINAL DETERMINATION OF WHETHER A BUSINESS ASSOCIATE AGREEMENT (BAA) IS NEEDED WITH A THIRD-PARTY VENDOR?



DISCUSSION:

- There are risks if vendors are not identified as business associates and agreements are not executed accordingly.
- A checklist to identify which vendors are BAs is helpful.
- It is a best practice that if the Privacy Officer is not a decision maker, they serve as consultants to the decision maker to identify potential Business Associates.
- In many cases, this will be a straightforward determination, but in other cases, the privacy officer's expertise and knowledge will be invaluable.
- If a procurement/contracting department is making the determination, someone in the department should understand HIPAA.

STRATEGIC MANAGEMENT

Investigations, Breach Management and Audits

SAI360

HOW ARE MOST HIPAA PRIVACY INCIDENTS DETECTED?

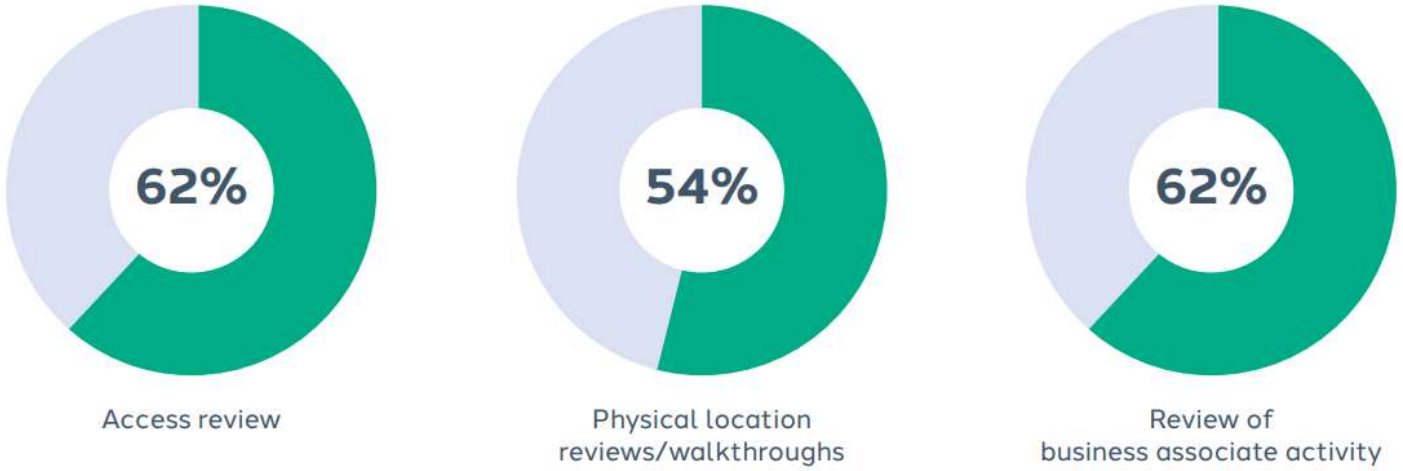
DISCUSSION:

WHAT WE FOUND:

The top five responses included (starting with the highest response):

1. Employee reports directly to management/HIPAA/Compliance Office — 84%
2. Monitoring of user access — 63%
3. Patient reports/complaints — 62%
4. Hotline reports — 62%
5. Reports from anonymous sources — 53%

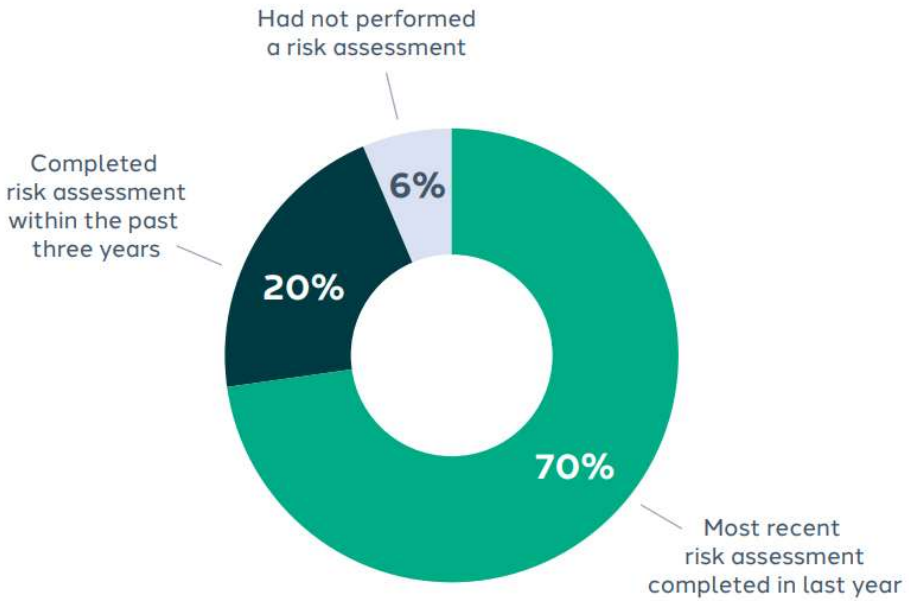
WHICH OF THE FOLLOWING ITEMS ARE CURRENTLY ON YOUR HIPAA/COMPLIANCE AUDIT WORK PLAN?



DISCUSSION:

- The responses continue to indicate that organizations have a wide variety of items and issues in their audit work plans.
- Best practices promote the use of audit work plans, but smaller organizations may not have the resources to complete a formal audit.
- Organizations should consider a more streamlined approach to auditing.

HIPAA REQUIRES PERFORMING A SECURITY RISK ANALYSIS TO IDENTIFY VULNERABILITIES THAT COULD RESULT IN A BREACH OF PHI.



DISCUSSION:

- Risk assessments are required.
- The rule does not specify the frequency of conducting the assessment.
- OCR guidance states that the “risk analysis process should be ongoing” and that covered entities may perform the assessment annually, bi-annually or every three years.
- If there is an incident, OCR investigators will most likely request data on the entity’s most recent risk assessment.

WHEN WAS THE LAST TIME YOUR ORGANIZATION HAD A HIPAA BREACH THAT HAS BEEN REPORTED TO THE OFFICE FOR CIVIL RIGHTS?

46%

Almost **46%** stated they reported a breach to OCR within the past year.

9%

About **9%** reported a breach within the past two years.

9%

Almost **9%** reported a breach between three and five years ago.

17%

Almost **17%** stated they had never had a breach reported to OCR.

DISCUSSION:

- In total, about 64% of respondents indicated that they experienced an OCR reportable HIPAA breach within the past five years.
- Almost 46% stated they reported a HIPAA breach within the last 12 months.
- It is nearly impossible to prevent all breaches.
- Training of the workforce/early detection of potential incidents with an immediate investigation followed by remediation as needed are key.
- Organizations should implement industry-accepted best practices to decrease the possibility of a data breach involving electronic PHI.

STRATEGIC MANAGEMENT

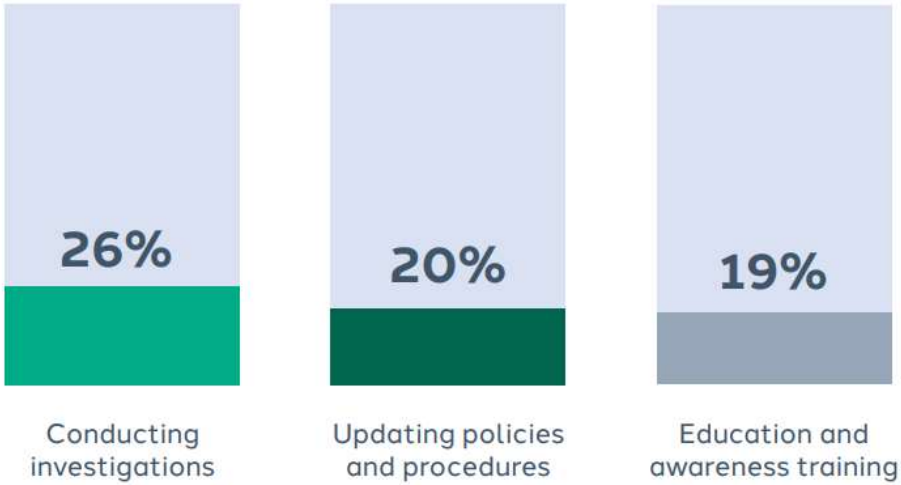
Program Planning Priorities and Resources

SAI360

PLEASE SELECT THE TOP THREE PRIORITIES TO BE ADDRESSED BY YOUR HIPAA COMPLIANCE PROGRAM IN THE NEXT 12 MONTHS

DISCUSSION:

WHICH OF THE FOLLOWING HIPAA RESPONSIBILITIES TAKES THE MOST PLANNING AND RESOURCES FOR YOUR ORGANIZATION?



DISCUSSION:

- Consistent with the 2023 Survey, conducting investigations took the most planning and resources.
- There was a slight decrease in the respondents who stated that updating policies and procedures took the most planning and resources.
- There was also a slight decrease in the respondents who stated that education and awareness took the most planning and resources.

WHAT TYPE OF SOFTWARE OR HARDWARE TOOLS DO YOU USE TO CARRY OUT THE PRIVACY PROGRAM OPERATIONS AT YOUR ORGANIZATION?

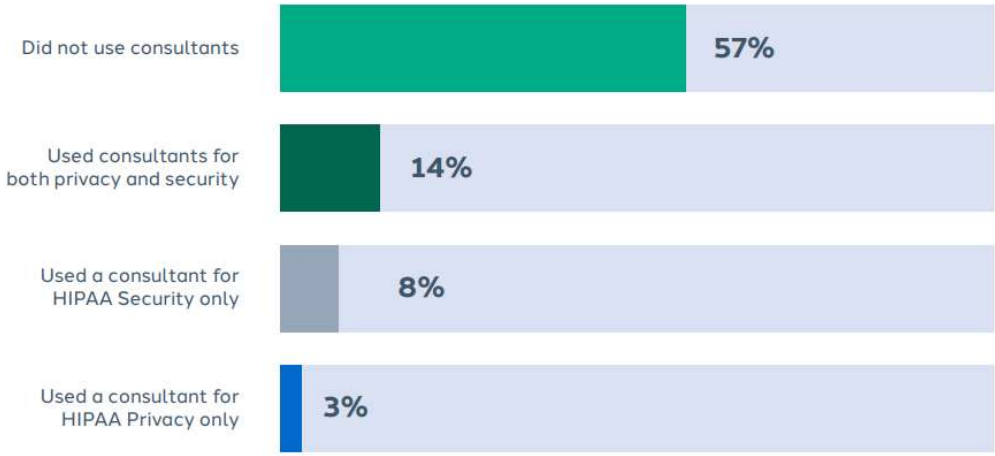
DISCUSSION:

- As with the prior survey, only a small number of organizations reported that they did not use any type of software for their Privacy Program operations.
- Software programs can help track investigations, train staff, and keep track of policies to ensure currency of the policy and facilitate access to the policies.
- A decrease in responses for every category indicate that not all organizations have the resources for elaborate expensive tools.
- Even using spreadsheets to track audits, policies, breaches, and training will provide the critical documentation to evidence an effective HIPAA compliance program.

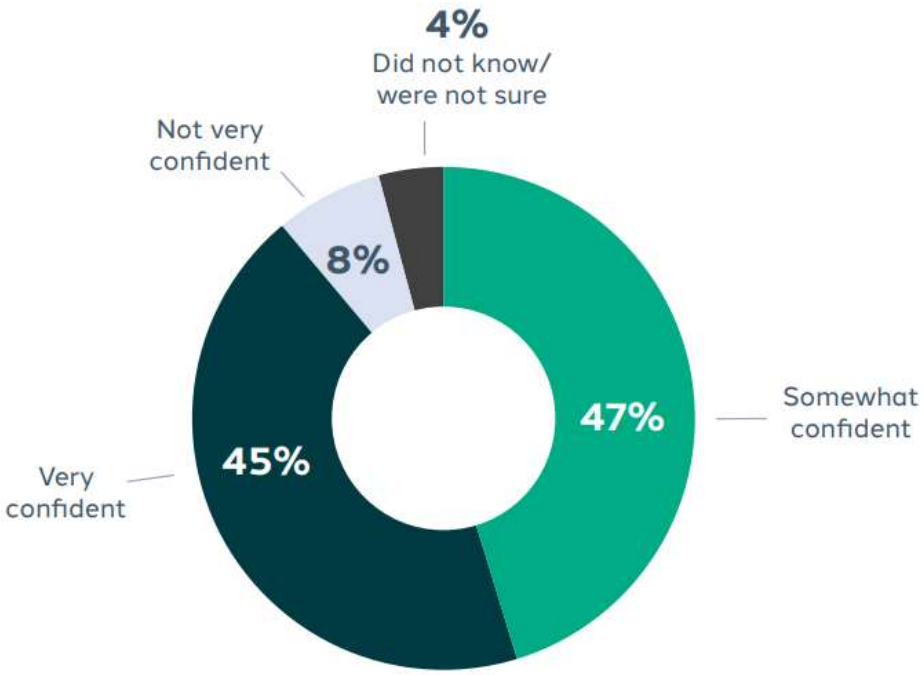
DOES YOUR ORGANIZATION USE ON-CALL CONSULTANT/VENDOR SERVICES TO ASSIST WITH HIPAA PRIVACY AND SECURITY FUNCTION

DISCUSSION:

- The responses to this year's survey are slightly lower than the 2023 survey results.
- The HIPAA Privacy and Security Rules do not require covered entities or business associates to use external vendors.
- These professionals can be helpful for tasks like breach investigations and conducting a HIPAA risk analysis.
- An on-call consultant can also help respond to independent audits or conduct research to resolve a complicated regulatory question.



HOW CONFIDENT ARE YOU THAT YOUR ORGANIZATION IS MEETING THE HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE REQUIREMENTS?



DISCUSSION:

- The percentage of respondents who are only “somewhat confident” was higher than those who were “very confident,” consistent with prior surveys.
- 4% of respondents indicated that they were not sure if their organization was meeting HIPAA regulatory requirements.

STRATEGIC MANAGEMENT

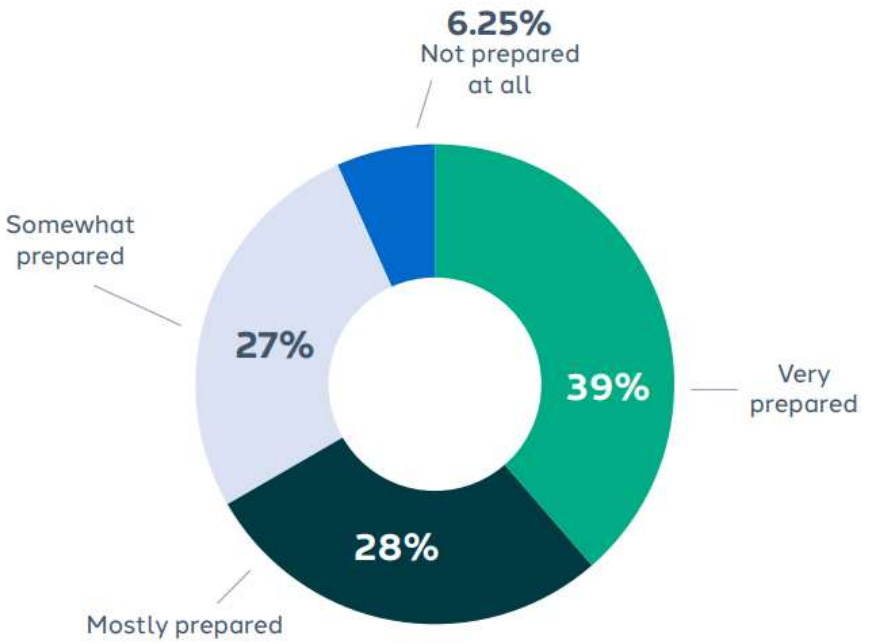
Enforcement

SAI360

HOW PREPARED IS YOUR ORGANIZATION FOR A HIPAA COMPLIANCE AUDIT OR INVESTIGATION FROM OCR?

DISCUSSION:

- The combined percentage of respondents who indicated they were “mostly” or “somewhat prepared” is a slight increase from the 2023 survey.
- The percentage of those stating that they were “very prepared” was 16% higher.
- The percentage stating they were “not prepared at all” was slightly lower.



WHEN WAS THE LAST TIME THE EFFECTIVENESS OF YOUR HIPAA PRIVACY PROGRAM WAS INDEPENDENTLY EVALUATED?

29%

Almost **29%** of respondents stated that an effectiveness evaluation had been performed within the last year.

12%

Almost **16%** had an evaluation conducted within the last three years.

43%

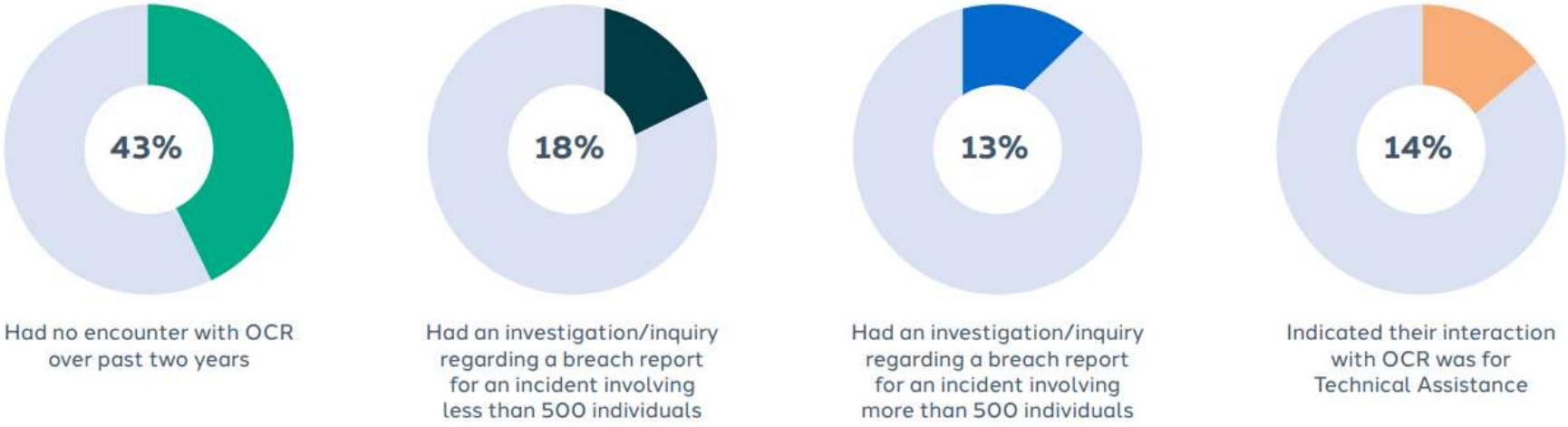
43% stated that either an evaluation had not been performed, or they were unsure of whether it had been performed.

DISCUSSION:

- Conducting an effectiveness evaluation within the past year follows a best practice for measuring compliance with the HIPAA Privacy Rule.
- The rule does not require covered entities to conduct independent reviews, but it is an important tool.
- An independent evaluation of the program may help organizations with small privacy and compliance workforces.
- Outside independent reviews are also helpful tools if an organization is going through a transition that may impact HIPAA privacy.

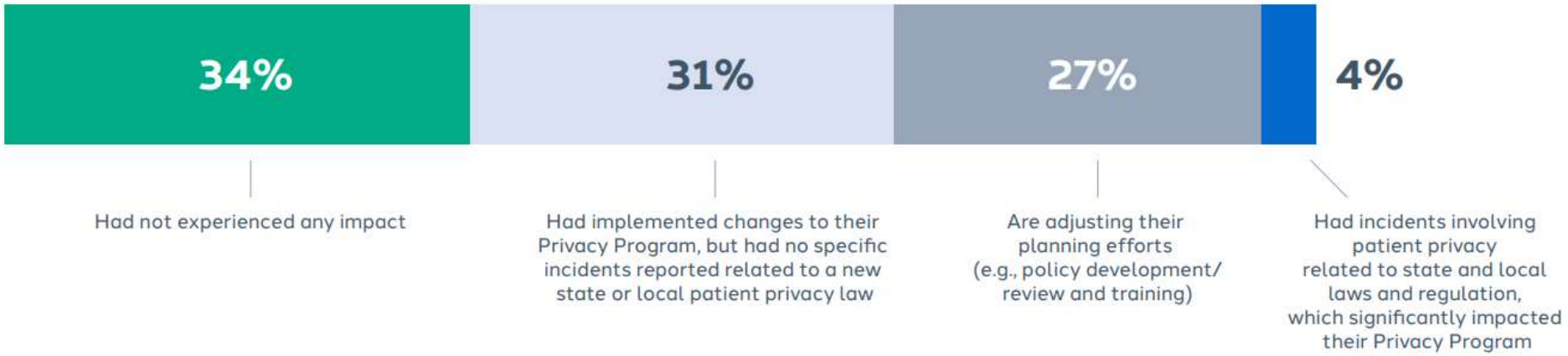
WHAT TYPE OF ENCOUNTERS HAS YOUR ORGANIZATION HAD WITH OCR IN THE LAST 2 YEARS?

DISCUSSION:



WHAT TYPE OF IMPACT HAS THE IMPLEMENTATION OF PATIENT PRIVACY-RELATED STATE AND LOCAL LAWS HAD ON YOUR PRIVACY PROGRAM?

DISCUSSION:



HAVE YOU BEGUN CHANGING YOUR NOTICE OF PRIVACY PRACTICES AND REVISING EXISTING OR CREATING NEW POLICIES AND OTHER DOCUMENTS TO REFLECT THE NEW REQUIREMENTS CONTAINED IN THE OCR'S LATEST FINAL RULE?

60%

A little more than **60%** of respondents indicated that they were waiting until we are closer to the February 2026 date.

40%

Almost **40%** of respondents indicated they had implemented changes.

DISCUSSION:

- It is best practice to implement changes to final rule requirements sooner rather than later.

- These updates should remain on Privacy Officer's work plans for implementation prior to the 2026 effective date.

OVERALL CONCLUSIONS

- There was a marked increase in the percentage of respondents representing behavioral mental health entities, which may indicate an increasing recognition of the importance of safeguarding patient privacy for those with mental health and substance use disorders in accordance with the Privacy Rule.
- Most Privacy Officers are reporting to the CEO or Compliance Officer and are providing formal reports to the Board of Directors and the Executive-Level Compliance Committee.
- Most organizations appear to have implemented operations to address HIPAA requirements.
- Most organizations are auditing a variety of items and issues and feel mostly or somewhat prepared for an OCR audit or investigation.

STRATEGIC MANAGEMENT

QUESTIONS?

SAI360

Thank you!

Robbi-Lynn Watnik

Senior Consultant, Strategic Management Services

rwatnik@strategicm.com

Natalie Lesnick

Consultant, Strategic Management Services

nlesnick@strategicm.com

STRATEGIC MANAGEMENT

Compliance.com

SAI360

sai360.com